Homeland Security

Daily Open Source Infrastructure Report
14 April 2015

Top Stories

- Miami officials reported April 9 that 42 individuals were charged in connection to various schemes in which the suspects allegedly used thousands of stolen identities to try to collect about $22 million in tax refunds and other benefits. – *Miami Herald* (See item **4**)

- Authorities arrested and charged a Kansas man April 10 for planning a suicide bomb attack against the Fort Riley military base in an alleged plan to support the Islamic State (ISIS). – *CBS News; Associated Press* (See item **18**)

- U.S. and European agencies along with private security firms collaborated with Interpol to disrupt the Simda botnet by seizing 14 command and control (C&C) servers throughout the Netherlands, U.S., Poland, Luxembourg, and Russia. – *Securityweek* (See item **21**)

- U.S. Department of Agriculture officials announced April 9 that $73 million will be invested to rehabilitate and assess about 150 dams in 23 States to consider structural integrity, flood damage protection, and water supply improvements. – *U.S. Department of Agriculture* (See item **31**)

Fast Jump Menu

PRODUCTION INDUSTRIES	**SERVICE INDUSTRIES**
• Energy	• Financial Services
• Chemical	• Transportation Systems
• Nuclear Reactors, Materials, and Waste	• Information Technology
• Critical Manufacturing	• Communications
• Defense Industrial Base	• Commercial Facilities
• Dams	**FEDERAL and STATE**
SUSTENANCE and HEALTH	• Government Facilities
• Food and Agriculture	• Emergency Services
• Water and Wastewater Systems	
• Healthcare and Public Health	

Energy Sector

Nothing to report

[Return to top]

Chemical Industry Sector

See item **5**

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

1. *April 11, Wilmington Star-News* – (North Carolina) **Brunswick reactor back at work after refueling.** Duke Energy officials reported that Brunswick Nuclear Generating Station's Unit 2 reactor in Southport was operating at 95 percent capacity April 10, following testing and a restart April 5 after the plant was taken offline February 20 for biannual refueling. Technicians replaced components in the reactor pressure vessel and completed post-Fukushima modifications required by the U.S. Nuclear Regulatory Commission during the outage.
Source: http://www.starnewsonline.com/article/20150411/articles/150419958

2. *April 11, PPL Susquehanna LLC; PR Newswire* – (Pennsylvania) **Unit 2 at Susquehanna Nuclear Power Plant begins scheduled refueling outage.** PPL Susquehanna LLC announced April 10 that operators had disconnected the Berwick-based Susquehanna Steam Electric Station's Unit 2 reactor from the electrical grid to replace approximately 40 percent of its uranium fuel, upgrade technology, and perform other maintenance as part of a scheduled outage. Unit 1 continues to operate at full power.
Source: http://www.prnewswire.com/news-releases/unit-2-at-susquehanna-nuclear-power-plant-begins-scheduled-refueling-outage-300064444.html

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

See item **22**

[Return to top]

Financial Services Sector

3. *April 10, Mount Pleasant Morning Sun* – (Michigan) **Mt. Pleasant woman admits opening fake accounts, stealing cash at Alpena bank.** A former branch manager and personal banker at Citizens Bank in Alpena pleaded guilty to embezzlement and filing false tax returns April 9 after a U.S. Internal Revenue Service investigation revealed that she allegedly stole over $300,000 from 2010 – 2011 by opening bank accounts in fictitious names and transferred funds to them from certificates of deposit held by elderly and deceased customers.
Source: http://www.themorningsun.com/general-news/20150410/mt-pleasant-woman-admits-opening-fake-accounts-stealing-cash-at-alpena-bank

4. *April 9, Miami Herald* – (National) **Feds bust 40 suspects in ID theft-fraud takedown in South Florida.** Miami officials reported April 9 that 42 individuals were charged in connection to various identity-tax refund, credit card, debit card, and Social Security fraud schemes in which the suspects allegedly used thousands of stolen identities to try to collect about $22 million in tax refunds and other government benefits from the U.S. Department of the Treasury, Florida, and other States. The suspects were paid out $3.2 million through the schemes.
Source: http://www.miamiherald.com/news/local/crime/article17932964.html

Transportation Systems Sector

5. *April 13, WRDW 12 Augusta* – (South Carolina) **Norfolk Southern says track is open again after Trenton train derailment.** A spokesman from Norfolk Southern reported April 12 that the track was reopened and that all evacuees had returned to their homes following a 36 car derailment that occurred when a train carrying ammonium nitrate and anhydrous ammonia stuck a downed tree and skipped the track near Salters Pond Road at Highway 121 in Trenton April 10, prompting an evacuation of approximately several homes in the surrounding area.
Source: http://www.wrdw.com/home/headlines/Law-enforcement-on-scene-of-train-derailment-in-Trenton-299420401.html

6. *April 13, South Florida Sun-Sentinel* – (Florida) **Four killed in plane crash near Fort Lauderdale Executive Airport.** Federal Aviation Administration officials reported that four people were killed when a twin-engine Piper Navajo plane crashed into a nature preserve as it was flying into the Fort Lauderdale Executive Airport in Florida after declaring an emergency April 12. The airport remained open but one runway was closed due to its proximity to the crash site.
Source: http://www.sun-sentinel.com/local/broward/fl-fort-lauderdale-plane-on-fire-20150412-story.html

7. *April 13, WYFF 4 Greenville* – (South Carolina) **Troopers: One dead, 5 injured in crash in Upstate.** Interstate 26 at mile marker 2 in Spartanburg County reopened after being closed for more than 3 hours April 13 while crews cleared the scene of a single-

vehicle accident that killed 1 person and injured 5 others.
Source: http://www.wyff4.com/news/fatal-wreck-blocks-i26-in-spartanburg-co/32334726

8. *April 12, Associated Press* – (Idaho) **Utahn among 4 dead in Idaho crash.** Custer County officials reported that four men were killed in a single-engine plane crash at the Loon Creek Airstrip near Challis, Idaho April 10. The cause of the crash remains unknown and the Federal Aviation Administration is investigating.
Source: http://www.sltrib.com/home/2390675-155/story.html

9. *April 11, Associated Press* – (Ohio) **2 arrested after bus bomb threat shuts down I-90 in Ohio.** Ohio State troopers reported that 2 Greyhound passengers were arrested April 10 after they made bomb threats while onboard the bus on its route from Buffalo, New York to Cleveland, prompting authorities to shut down Interstate 90 outside of Cleveland for about 3 hours to investigate the scene. No explosives were found and the bus continued on its route.
Source: http://www.whio.com/ap/ap/ohio/2-arrested-after-bus-bomb-threat-shuts-down-i-90-i/nkrnX/

[[Return to top]]

Food and Agriculture Sector

10. *April 11, U.S. Department of Agriculture* – (California) **Corn Maiden Foods, Inc. recalls beef and pork products due to misbranding and an undeclared allergen.** The Food Safety and Inspection Service announced April 11 that Corn Maiden Foods, Inc., recalled about 15,600 pounds of pork tamales pork Yucatan, and beef brisket taquitos products due to misbranding and undeclared hydrolyzed soy protein. The recalled products were distributed to hotels, restaurants, and institutional locations in California.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-059-2015-release

11. *April 10, U.S. Food and Drug Administration* – (Connecticut; Maryland) **Cargill recalls beef products due to possible foreign matter contamination.** The Food Safety and Inspection Service announced April 10 that Cargill Meat Solutions issued a recall for about 8,294 pounds of Meadowland Farms Ground Beef product after a cotton/poly blend blue string was found in one of the establishment's machines during routine cleaning processes. The recalled items were shipped to warehouse locations in Connecticut and Maryland.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/rnr-058-2015

12. *April 10, Mississippi News Now* – (Mississippi) **200 workers at chicken plant to be tested for tuberculosis.** The Mississippi Department of Health will be administering blood tests to 200 workers at the PECO Foods chicken plant in Canton April 14 after a former employee tested positive for Tuberculosis. Officials stated there is no public

health risk associated with the incident.
Source: http://www.msnewsnow.com/story/28772118/exclusive-state-health-dept-confirms-case-of-tuberculosis

Water and Wastewater Systems Sector

13. *April 13, St. Louis Post-Dispatch* – (Missouri) **Boil water advisory in north St. Louis County expected to continue until Tuesday.** Missouri American Water issued a precautionary boil water advisory for customers in parts of north St. Louis County April 11 following a water main break, and reported that the advisory is expected to continue until April 14.
Source: http://www.stltoday.com/news/local/metro/boil-water-advisory-in-north-st-louis-county-expected-to/article_306c716a-c575-559e-a7ce-3403de51a2e3.html

Healthcare and Public Health Sector

14. *April 11, Los Angeles Times* – (Indiana) **Rural Indiana HIV outbreak spreads to more than 100 cases.** The Indiana health commissioner reported 95 confirmed cases and 11 preliminary cases of HIV April 11 in the southeast portion of the State, up from the more than 70 previously confirmed cases. The spread of the virus was linked to the use of contaminated syringes and the use of the painkiller Opana, prompting the governor to declare a state of emergency and authorize a short-term needle exchange in March.
Source: http://www.latimes.com/nation/la-na-indiana-hiv-20150411-story.html

Government Facilities Sector

15. *April 13, NBC News* – (North Carolina) **Wayne Community College in North Carolina on lockdown after deadly shooting.** Officials reported April 13 that one Wayne Community College employee was killed after being shot near the general library area, prompting the North Carolina campus to go on lockdown while police searched for the gunman who was believed to be a former student. The college was closed and all classes and activities were canceled for the remainder of the day.
Source: http://www.nbcnews.com/news/us-news/north-carolinas-wayne-community-college-lockdown-after-shooting-reports-n340551

16. *April 13, Boston Globe* – (Massachusetts) **Two Mass. high schools close Monday due to bomb threats.** Whitman-Hanson Regional High School and Brockton High School in Massachusetts were both closed April 13 due to bomb threats. Police were conducting searches of the buildings and buses and classes were expected to resume April 14.

Source: http://www.bostonglobe.com/metro/2015/04/13/mass-high-schools-close-monday-due-bomb-threats/oUYjpasCGqbt3CErrcBltJ/story.html

17. *April 11, WIAT 42 Birmingham* – (Alabama) **School bus driver dies after serious accident in Pickens County.** A school bus driver was killed and 16 people, including 14 students, were injured after the school bus collided with a vehicle, ran off the roadway, and struck a tree in Pickens County April 10.
Source: http://wiat.com/2015/04/11/school-bus-driver-dies-after-serious-accident-in-pickens-county/

18. *April 10, CBS News; Associated Press* – (Kansas) **Kansas man accused of suicide plot at Army base.** Authorities arrested and charged a Kansas man April 10 for planning a suicide bomb attack against the Fort Riley military base in an alleged plan to support the Islamic State (ISIS), after the suspect attempted to arm what he thought was a 1,000-pound bomb inside a van near the base. Federal prosecutors claimed that the suspect met with an undercover FBI agent in October 2014 and expressed extremist views and a desire to attack American soldiers.
Source: http://www.cbsnews.com/news/john-booker-army-recruit-in-kansas-accused-of-trying-to-support-isis/

19. *April 10, WFAA 8 Dallas* – (Texas) **22 evaluated for nausea, vomiting at Fort Worth school.** Fifteen students and adults were evaluated by medical staff as a precaution after a teacher at Diamond Hill Elementary School in Fort Worth complained of nausea and dizziness April 10. The school was briefly evacuated while firefighters checked for carbon monoxide and other fumes, and officials stated that the district will monitor the air in the building through April 13.
Source: http://www.wfaa.com/story/news/local/tarrant-county/2015/04/10/fort-worth-diamond-hill-elementary-school-nausea-vomiting/25582515/

For another story, see item **22**

Emergency Services Sector

20. *April 10, WCSH 6 Portland* – (Maine) **Police departments hit by ransomware virus.** The Lincoln County Sheriff's Office in Maine reported that an employee inadvertently downloaded ransomware dubbed megacode, which encrypted all computer data on a shared network, affecting four towns and the county. The county paid a ransom fee of $300 to the creator of the virus which unlocked and restored the data.
Source: http://www.wcsh6.com/story/news/local/2015/04/10/police-departments-hit-by-ransomware-virus/25593777/

For another story, see item **26**

Information Technology Sector

21. *April 13, Securityweek* – (International) **Law enforcement, security firms team up to disrupt Simda botnet.** U.S. and European agencies along with private security firms collaborated with Interpol to disrupt the Simda botnet by seizing 14 command and control (C&C) servers throughout the Netherlands, U.S., Poland, Luxembourg, and Russia. The malware is usually delivered via exploit kits (EK) and is often used for the distribution of malware and potentially unwanted applications (PUA), and has infected over 770,000 computers worldwide over the past 6 months.
Source: http://www.securityweek.com/law-enforcement-security-firms-team-disrupt-simda-botnet

22. *April 12, IDG News Service* – (International) **Chinese hacker group among first to target networks isolated from internet.** FireEye released findings in a technical report that identify a hacker group called Advanced Persistent Threat (APT) 30 as one of the first to target air-gapped networks with malware that has infected defense-related clients' systems worldwide, utilizing custom-made malware components with worm-like capabilities that can infect removable drives such as USB sticks and hard drives.
Source: http://www.networkworld.com/article/2909093/chinese-hacker-group-among-first-to-target-networks-isolated-from-internet.html

23. *April 11, Softpedia* – (International) **New Shellshock worm seeks vulnerable systems at tens of thousands of IPs.** Security researchers at Volexity observed that cybercriminals had amassed 26,356 internet protocol (IP) addresses belonging to systems vulnerable to the Shellshock bug for the Bash command shell found in many Linux and Unix systems, that allows attackers to execute arbitrary commands by appending them after a variable function. Scanning for vulnerable systems has since decreased and the malicious files were removed from the IP address hosting them.
Source: http://news.softpedia.com/news/New-Shellshock-Worm-Seeks-Vulnerable-Systems-at-Tens-of-Thousands-of-IPs-478233.shtml

24. *April 10, Krebs on Security* – (International) **Don't be fodder for China's 'Great Cannon'.** Researchers from the University of Toronto, the International Computer Science Institute, and the University of California, Berkeley, released findings that a percentage of unencrypted Web traffic destined for the Chinese search service Baidu was actively manipulated by censors via malicious JavaScript (JS) files to cause users' browsers to participate in denial-of-service (DoS) attacks. The capability was dubbed "The Great Cannon" and could serve malicious code that exploits other browser vulnerabilities.
Source: http://krebsonsecurity.com/2015/04/dont-be-fodder-for-chinas-great-cannon/

25. *April 10, Securityweek* – (International) **Siemens patches DoS, other vulnerabilities in SIMATIC HMI products.** Siemens began releasing security updates addressing several vulnerabilities in its SIMATIC HMI (human-machine interaction) devices which include allowing attackers positioned between the HMI panel and programmable logic controller (PLC) to cause a denial-of-service (DoS) condition and intercept or modify industrial communication by sending specially crafted packets on transmission

control protocol (TCP) port 102. Additional vulnerabilities include the ability to launch a man-in-the-middle (MitM) attack, and a flaw that allows users to authenticate themselves with password hashes instead of full passwords.
Source: http://www.securityweek.com/siemens-patches-dos-other-vulnerabilities-simatic-hmi-products

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

[Return to top]

Communications Sector

26. *April 10, San Francisco Bay City News* – (National) **Sprint agrees to pay $15.5M in Federal surveillance lawsuit.** Authorities announced April 9 that Sprint Communications, Inc., had agreed to pay $15.5 million to settle allegations that the company defrauded Federal law enforcement agencies out of $21 million from 2007 to 2010 by billing for expenses not covered under the Communications Assistance in Law Enforcement Act, while recovering otherwise legitimate costs of carrying out court-ordered wiretaps and surveillance activities.
Source: http://sfappeal.com/2015/04/sprint-agrees-to-pay-15-5m-in-federal-surveillance-lawsuit/

[Return to top]

Commercial Facilities Sector

27. *April 13, WTSP 10 St. Petersburg; Associated Press* – (Florida) **Crash at Disney World auto racing attraction kills 1.** The driver of a car at the Exotic Driving Experience auto racing attraction at the Disney World amusement park in Florida lost control of the vehicle on the attraction's course and crashed into a guardrail April 11, killing a passenger and injuring the driver.
Source: http://www.wtsp.com/story/news/local/2015/04/12/fatal-crash-at-richard-petty-experience/25684239/

28. *April 12, Associated Press* – (Virginia) **Car smashes into Annandale bakery, injuring 6.** Six people were injured April 12 when a car crashed into the storefront of Napoleon Bakery in Annandale. The bakery is closed until further notice pending an inspection to determine the structural integrity of the building.
Source: http://www.wjla.com/articles/2015/04/car-smashes-into-annandale-bakery-injuring-6-113105.html

29. *April 10, WROC 8 Rochester* – (New York) **HAZMAT situation causes Holiday Inn**

to be evacuated. All guests at a Holiday Inn hotel in Henrietta were evacuated and relocated to a different hotel after a chemical fog was discovered in the business' basement April 10. A HAZMAT team responded to the scene.
Source: http://www.rochesterhomepage.net/story/d/story/hazmat-situation-causes-holiday-inn-to-be-evacuate/37622/gsB7xUSnn0K_8oIH_18XiA

30. *April 10, WMTW 8 Poland Spring* – (Maine) **$40,000 in copper stolen from Great Falls Balloon Festival.** Organizers of the Great Falls Balloon Festival in Maine reported that about $40,000-50,000 worth of copper power cords were stolen from a storage trailer between October 2014 and January 2015. The festival grounds at Simard-Payne Memorial Park cannot open until the cords are replaced to provide electricity.
Source: http://www.wmtw.com/news/40000-in-copper-stolen-from-great-falls-balloon-festival/32298050

[Return to top]

Dams Sector

31. *April 9, U.S. Department of Agriculture* – (National) **USDA invests in critical dam rehabilitation and assessment projects in 23 states.** U.S. Department of Agriculture officials announced April 9 that $73 million will be invested to rehabilitate and assess about 150 dams in 23 States to consider structural integrity, flood damage protection, and water supply improvements.
Source:
http://www.usda.gov/wps/portal/usda/usdahome?contentid=2015/04/0092.xml&contentidonly=true

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.